DROIT À L'IMAGE ET À L'OUBLI

Droit à l'image

Vous avec un droit sur l'utilisation et la diffusion de votre image, c'est une donnée personnelle, vous pouvez vous opposer à sa conservation ou sa diffusion publique sans votre autorisation.
Il existe quelques cas particuliers :
- photographies durant l'exercice d'une fonction d'une personnalité publique,
- photographies relevant du droit à l'information.

Toute atteinte au droit à l'image constitue une violation de la vie privée et vous êtes en droit de saisir un tribunal civil ou pénal, ou la CNIL.

Droit à l'oubli

Internet conserve tout : ce que vous avez publié hier, mais aussi ce que vous avez publié il y a 15 ans. Vous avez mûri, changé d'activité, de vie, de profession, êtes victimes de harcelement électronique, et vous ne souhaitez pas conserver ces informations obsolètes.
Il est aujourd'hui pratiquement impossible de supprimer ces anciennes publications si elles sont hébergées sur des sites que vous ne contrôlez pas. Malgré les évolutions de la législation Européenne et Française sur le sujet ("droit à l'oubli"), la mise en œuvre de ces processus est généralement complexe, et reste soumise au bon vouloir de l'hébergeur.
C'est par exemple le cas avec Google, qui dispose d'un dispositif permettant de demander le retrait des informations publiées, mais reste seul juge d'accepter ou non cette demande.

Plus d'informations sur :
- http://www.francetvinfo.fr/internet/google/j-ai-teste-pour-vous-le-formulaire-de-droit-a-l-oubli-de-google_610473.html
- https://support.google.com/legal/contact/lr_eudpa?product=websearch

RESSOURCES

Reprendre en main ses données : https://controle-tes-donnees.net/
Guide d'autodéfense numérique : https://guide.boum.org/
La Quadrature du net : https://www.laquadrature.net/fr/Vie_privee
La CNIL : https://www.cnil.fr/

Retrouvez plus de ressources sur le site https://cafevieprivee-nantes.fr

Document réalisé par l'association

Faimaison

GUIDE PRATIQUE

COMMENT PROTÉGER SA VIE PRIVÉE EN LIGNE ET SES DONNÉES PERSONNELLES ?

POURQUOI PROTÉGER SA VIE PRIVÉE ET SES DONNÉES ?

Sur Internet vous laissez des traces, de toutes sortes : adresses IP, adresses mails, comptes sur les réseaux sociaux et publication, pages web visitées, achats réalisés, etc. Toutes ces données peuvent servir à dresser votre profil, vos habitudes, pour mieux cibler vos attentes.
Ces données se monnayent, elles peuvent aussi être piratées et divulguées car vous pouvez être la victime de négligences, d'attaques, de cyber-harcèlement.

Même si vous pensez ne rien avoir à cacher de particulier, vous souhaitez surement préserver votre intimité, ne pas vouloir que l'on connaisse tout ce que vous faîtes sur Internet ou avec qui vous communiquez. Pour éviter cela, quelques bonnes pratiques sont proposées dans ce document.

COMMENT SE PROTÉGER ?

La protection de sa vie privée et de ses données sur Internet peut prendre plusieurs formes et différents niveaux. Cela peut aller de la vigilance lors de l'utilisation d'outils en lignes et des traces que l'on laisse, à la volonté de maîtriser son identité numérique.

UTILISER DES ALTERNATIVES LOGICIELLES

NAGIVATION SUR INTERNET

Navigateurs web

- Firefox
- Chromium
- TorBrowser

Extensions pour la navigation

- Do Not Track Plus
- Disconnect
- uBlock Origin (bloque les publicités)
- HTTPS Everywhere (HTTPS automatique pour les sites visités)
- NoScript (désactive le Javascript)
- Privacy Badger (bloque les publicités et les trackers)

Moteurs de recherche

- DuckDuckGo
- Searx
- Search.disconnect.me

MESSAGERIE

Hébergeur de mails

- Mailoo
- Riseup
- Autohébergement

Clients mail / Web mail

- Thunderbird / Icedove
- RoundCube

CARTOGRAPHIE

- OpenStreetMap

OUTILS COLLABORATIFS

- FramaPad (traitement de texte partagé)
- FramaDate (sondage)
- Framacalc (tableur partagé)

GÉRER SES MOTS DE PASSE

Afin de vous aider à stocker et gérer vos mots de passe, vous pouvez utiliser un logiciel tel que KeepassX.
Tous vos mots de passe se retrouvent dans une base de données, qui peut être sauvegardée sur un support extérieur que votre ordinateur.

Quelques rappels sur les bonnes pratiques :
- utiliser une phrase de passe forte pour votre gestionnaire de mots de passe
- utiliser des mots de passe générés pour tous vos services : mail, accès à sa banque, accès aux réseaux sociaux, etc.
- sauvegarder régulièrement votre fichier de mots de passe

CHIFFRER SES COMMUNICATIONS

L'objectif du chiffrement de ses mails est de protéger votre vie privée, ainsi que celle des personnes avec qui vous communiquez par messagerie.
Il existe un guide en ligne très détaillé pour apprendre à chiffrer ses mails avec PGP : https://emailselfdefense.fsf.org/fr/
La durée de mise en place des outils avec ce guide prend environ 40 minutes.

Il est également possible de chiffrer ses SMS et MMS avec les applications Silence ou Signal. Les échanges sont ainsi protégés de bout en bout entre les utilisateurs de l'application.

CHIFFRER SON TRAFIC AVEC UN VPN

Un VPN est un réseau privé virtuel, il crée un tunnel chiffré entre vous et votre fournisseur de VPN. Il permet ainsi de sécuriser son accès Internet sur un réseau non fiable, par exemple un réseau WiFi public ou un réseau d'un FAI auquel vous ne faîtes pas confiance, etc.
Vous pouvez souscrire à un abonnement VPN auprès de FAI de la fédération FFDN ou auprès d'autres structures (entreprises, associations).

PROTÉGER SON ANONYMAT AVEC TAILS ET TOR

Tails est un système d'exploitation qui fonctionne sur clé USB. Il est utile lorsque vous voulez utiliser un ordinateur qui n'est pas le votre et si vous n'avez pas confiance dans le système installé et les données qui peuvent y être conservées. Ainsi Tails vous permettra de rester anonyme, notamment en faisant transiter toutes vos communications via le réseau Tor, masquant ainsi votre IP réelle.

Il est aussi possible d'utiliser Tor sans Tails en naviguant sur Internet avec le TorBrowser (réalisé avec le navigateur Firefox).